



Defendants concealed a critical ransomware attack, misrepresented their operational readiness and data security compliance, and failed to fulfill their obligations under multiple agreements with Plaintiff BEN and Due Figlie. Through this misconduct, Defendants unjustly enriched themselves, caused significant financial harm to Plaintiff, and jeopardized Plaintiff's business relationships, reputation, and strategic initiatives. Plaintiff now seeks to hold Defendants accountable for their actions and recover damages for the harm caused.

## **I. PARTIES**

1. BEN is a publicly traded corporation incorporated in Delaware with its principal offices in Jackson, Wyoming and Seoul, Republic of Korea. BEN is an innovator in AI-powered customer engagement solutions, providing advanced technology designed to enhance data utilization, improve customer interactions, and drive operational efficiency. BEN entered into the Exclusive Reseller Agreement with AFG Companies Inc., ("AFG") as part of its strategy to expand into the automotive market. BEN has been assigned all claims to pursue this action by Due Figlie as elaborated on above.

2. Defendant Ralph Wright Brewer III is an individual residing in Bartonville, Texas, and serves as the Chairman and CEO of AFG Companies Inc. Brewer is the architect of the fraudulent schemes and bad faith actions described in this lawsuit, acting personally and through the AFG entities to misrepresent material facts, conceal a significant ransomware attack, and enrich himself at the expense of BEN and Due Figlie.

3. Brewer exercised complete control over the AFG entities, disregarding corporate formalities and using the entities as his alter ego to commit fraud and evade contractual obligations. Brewer's misconduct demonstrates personal liability under theories of fraud, securities violations, and piercing the corporate veil.

4. Defendant Automotive Financial Group, Inc. (AFG) is a Texas domestic for-profit corporation with its principal place of business in Grapevine, Texas. AFG was the primary counterparty to the Exclusive Reseller Agreement and failed to fulfill its contractual obligations by concealing the ransomware attack and breaching its data security and performance requirements.

5. Defendant AFG Companies, Inc. is a Texas domestic for-profit corporation that played a key role in facilitating the misconduct alleged in this lawsuit. It participated in misrepresenting AFG's compliance and performance during negotiations and actively benefited from the fraudulent actions described herein.

6. AFG Technologies, LLC d/b/a Tronix, is a Texas limited liability company focused on developing and delivering technology solutions for the automotive industry. This entity directly participated in the misrepresentations and omissions made during the negotiation of the Exclusive Reseller Agreement, particularly regarding data security and operational readiness.

7. CareGard Warranty Services, Inc. is a Texas corporation specializing in automotive warranty services. CareGard was a key party in the Due Figlie Consulting Agreements, which required payment of an Agent Fee for new business generated by Due Figlie and good faith negotiations regarding equity compensation in connection to the technology product known as Tronix. CareGard's failure to honor these agreements caused significant harm to Due Figlie.

8. Southwest Colonial Reinsurance, Ltd. is a reinsurance entity affiliated with the AFG entities that resides in Texas. This entity was instrumental in managing financial transactions and reinsurance programs related to the misconduct alleged herein. Its involvement ties it directly to the financial harm caused to BEN and Due Figlie.

9. Defendant Prime Reserve Plus, Inc. is a Texas corporation engaged in financial activities tied to the AFG entities. It acted in concert with Brewer and the other defendants to facilitate the fraudulent schemes described in this lawsuit.

10. Defendant DaidaX, Inc., formerly known as Pathwai, Inc. and Ben Automotive, Inc. is a Texas Corporation engaged in software technology and a subsidiary of AFG. It acted in concert with Brewer and other defendants to facilitate the fraudulent schemes described in this lawsuit.

11. Defendant DeLaporte Learning, Inc. is a Texas corporation that is controlled by Brewer and AFG. It acted in concert with Brewer and other defendants to facilitate the fraudulent schemes described in this lawsuit.

12. BEN brings this action not only on its own behalf but also on behalf of its shareholders as well as on behalf of Due Figlie, LLC (“Due Figlie”), pursuant to a valid and enforceable Claims Assignment Agreement (the “Agreement”) executed between the parties, effective January 14, 2025.

13. Under the Agreement, Due Figlie assigned to BEN to a portion of its claims against AFG Companies, Inc. and its affiliates, as well as against Ralph Wright Brewer III arising from breaches of contractual obligations owed to Due Figlie, including but not limited to its ownership percentage in AFG and unpaid agent fees and bonuses.

14. The claims assigned to BEN are directly related to the fraudulent and deceptive conduct engaged in by AFG and Brewer and arise from the same nexus of facts, including the misrepresentation of AFG’s value, wrongful denial of contractual payments owed to Due Figlie, and other acts of bad faith. BEN seeks to recover all damages owed to Due Figlie and itself as a result of Defendants’ wrongful actions.

## II. JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331, as Plaintiff asserts claims arising under federal law, including violations of the Securities Exchange Act of 1934, Section 10(b) (15 U.S.C. § 78j(b)), and Rule 10b-5 promulgated thereunder. Defendants engaged in fraudulent conduct and deceptive practices in connection with the purchase or sale of securities, including stock and warrant agreements issued to Defendant Brewer and his affiliated entities.

16. This Court also has jurisdiction under 28 U.S.C. § 1332(a), as there is complete diversity of citizenship between Plaintiff BEN and Defendants, and the amount in controversy exceeds \$75,000, exclusive of interest and costs.

17. Plaintiff BEN is a citizen of Delaware and Wyoming, while the Defendants are citizens of Texas. The corporate defendants, including Automotive Financial Group, Inc., AFG Companies, Inc., AFG Technologies, LLC, CareGard Warranty Services, Inc., Southwest Colonial Reinsurance, Ltd., DeLaPorte Learning Inc., Prime Reserve Plus, Inc. and DaidaX, Inc. formerly known as Pathwai Inc and Ben Automotive, Inc., are all Texas entities. Defendant Brewer is an individual residing in Texas.

18. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367, as these claims are so closely related to the federal claims that they form part of the same case or controversy under Article III of the United States Constitution.

19. Venue is proper in the Northern District of Texas, Dallas Division, pursuant to 28 U.S.C. § 1391(b), because:

- i. The Exclusive Reseller Agreement between BEN and AFG Companies, Inc. expressly designates Dallas, Texas, as the venue for resolving disputes arising under the Agreement.

- ii. A substantial part of the events or omissions giving rise to the claims occurred in this District, including Defendants' execution of the fraudulent Reseller Agreement, concealment of the ransomware attack, and repudiation of contractual obligations to Plaintiff and Due Figlie.
- iii. Defendants Brewer and the AFG entities conduct significant business operations in this District, including activities directly related to the claims in this action.

20. This Court has personal jurisdiction over all Defendants because they reside, are incorporated, or conduct substantial business in Texas, including within the Northern District of Texas. Defendant Brewer resides in Texas and personally participated in the misconduct alleged herein. The corporate defendants are Texas-based entities whose operations are central to the claims in this case. By entering into agreements with BEN, performing actions in furtherance of the fraudulent scheme, and breaching obligations in this District, Defendants purposefully availed themselves of the jurisdiction of this Court.

### **III. FACTUAL BACKGROUND**

#### **A. Brewers Scheme to Defraud BEN**

21. In the summer of 2023, Ralph Wright Brewer III devised and executed a calculated plan to defraud BEN of its proprietary technology, intellectual property, and substantial value in securities and stock. This scheme was characterized by deception, manipulation, and a flagrant disregard for ethical and legal obligations.

22. Brewer's duplicity extended to his own workforce, as evidenced by a lawsuit filed against an AFG employee, Sean Dawson ("Dawson"), alleging misconduct. Brewer would further go on to file lawsuits against Travis Gates, President of AFG Technologies. This lawsuit was part of Brewer's broader pattern of retaliatory actions and abuse aimed at consolidating control and suppressing dissent.

23. In December of 2023, Brewer testified under oath during a deposition in the Dawson suit that AFG was “worth nothing,” even going so far as to state that the company’s net worth was in the negative due to mounting financial losses. Despite this sworn testimony, Brewer had negotiated with BEN to sell AFG for the valuation of \$120 million—either in cash or in equivalent stock. These contradictory positions expose Brewer’s deliberate misrepresentation of AFG’s value and concealment of his financial situation to further his fraudulent objectives.

24. On March 7, 2024, Brewer convened a clandestine off-site executive meeting at 8343 Hilltop Road, Argyle, Texas ominously titled “AFG Executive Vision Meeting” to conspire with others to compete against BEN. During this meeting, Brewer unveiled a five-year plan centered on creating a new entity to compete against BEN, its new business partner, known as “Pathwai.” Specifically, Pathwai was designed to compete against BEN in the automotive AI market. Brewer openly declared “war on” BEN as AFG’s direct competition. This declaration came despite the fact that Brewer had already reaped significant personal financial gains from his BEN stock holdings. His calculated betrayal laid bare his intent to undermine BEN even as he grossly enriched himself to BEN’s detriment in the automotive market.

25. By March 15, 2024, Brewer’s scheme had reached its apex. BEN’s stock became publicly traded, instantly making Brewer and his family multimillionaires. On or about March 19, 2024, Brewer wasted no time capitalizing on his ill-gotten gains. Witnesses observed Brewer in his office, pressuring his Goldman Sachs stockbroker, Sean Baird, to liquidate as much BEN stock as possible at the market’s opening. Brewer acknowledged to the witness the sale of securities on Friday, March 15, 2024, the day BEN began trading on the NASDAQ. At this time, Brewer was an insider holding more than 7% of BEN’s stock, a fact he knowingly concealed from BEN, the

public markets, and the SEC in direct violation of securities laws. This concealment was integral to Brewer's fraudulent scheme, allowing him to profit while evading disclosure obligations.

26. While AFG/Brewer was cashing out their BEN stock, AFG under their own admission in the AFG Vision meeting, lacked the technological infrastructure, data, or platform necessary to fulfill its contractual obligations to BEN. Instead, Brewer focused his efforts on advancing Pathwai (known as DaidaX as of October 17, 2024) by developing a new AI platform the covert initiative designed to compete with BEN. In the March 7, 2024, AFG Vision meeting with key executives, one executive stated, "We are not communicating this, by the way outside of this room. We are not communicating this is we have to build this covertly with no one knowing for a while. Okay, we have to do it that way or we lose it's part of the strategic advantage." Within days of the AFG Vision meeting, Brewer had pocketed millions from his fraudulent sale of BEN stock, all while continuing to conceal the existence of building a competing AI platform to BEN. At the AFG Vision meeting on March 7, 2024, Brewer and his executive team plotted to directly compete with BEN. Another example is the statement from their executive, "could be we force the, you know, Drive Centric, to play or we pivot, that can be one, but eventually, they're all going to get wind and go, the only way we win is to keep those people locked out." AFG restricted BEN from accessing AFG data and did not provide an application program interface (API) to BEN, because in their own words, "keep those people locked out".

27. On or about May 9, 2024, Brewer and AFG took down the BEN Automotive website [www.benauto.ai](http://www.benauto.ai) and did not reactivate it until sometime recently in December of 2024 or January 2025. Neither Brewer or AFG notified BEN of their actions.

28. On or about June 28, 2024, AFG amended the name with the Texas Secretary of State of BEN Automotive, Inc. to Pathwai, Inc. This name amendment was not disclosed to BEN.



29. After the departure of another employee, and in order to further conceal their fraudulent scheme, on October 28, 2024, AFG filed another amended name with the Texas Secretary of State of Pathwai, Inc. to DaidaX, Inc., formerly known as BEN Automotive, Inc. originally filed with the Texas Secretary of State on December 22, 2023.

30. The scope of Brewer's duplicity became public in November 2024, when Maurice Fitzpatrick filed a motion to intervene in a matter currently pending before the 17<sup>th</sup> Judicial District court in Tarrant County, Texas cause number 017-352358-24 styled *AFG Companies, Inc., v. Genuine Lifetime, LLC, and Tyler J. Luck*. Fitzpatrick's filing included a damning recorded conversation between AFG's President Jason De Laporte and CTO David Dugan. In the recording, Dugan admitted that Pathwai was created to compete with BEN in the automotive AI market. A true and correct copy of the recorded conversation is attached hereto as **Exhibit A**. He further revealed that their actions were driven by a need to "protect the \$33 million" Brewer had fraudulently acquired through his manipulation of BEN stock.

31. Brewer's conduct demonstrates a premeditated conspiracy to defraud BEN, sabotage its position in the automotive AI market, and amass personal wealth at the company's expense. This fraudulent scheme has inflicted significant financial and reputational harm on BEN, and Brewer's actions demand full accountability under the law.

#### **B. The Exclusive Reseller Agreement**

32. On August 19, 2023, BEN, a cutting-edge innovator in AI-powered customer engagement solutions, entered into an Exclusive Reseller Agreement with AFG. A true and correct copy of the Exclusive Reseller Agreement is attached hereto as **Exhibit B**. This agreement represented a strategic partnership designed to integrate BEN's proprietary AI technology into

AFG's dealership systems. The collaboration aimed to revolutionize how dealerships utilize real-time data to enhance customer interactions and streamline their operations.

33. The Exclusive Reseller Agreement was a cornerstone of BEN's efforts to expand into the automotive sector, leveraging AFG's established presence and network within the industry. AFG was tasked with reselling BEN's AI technology as part of its product offerings to automobile manufacturers, distributors and franchise dealerships across the country. The success of this partnership was dependent on AFG's compliance with data security standards and operational readiness, which AFG and its CEO, Ralph Wright Brewer III, explicitly represented as being fully in place.

34. As part of the Exclusive Reseller Agreement, AFG was required to:

- i. Maintain strict compliance with all applicable state and federal laws, particularly those governing data privacy and cybersecurity.
- ii. Disclose any cybersecurity incidents or vulnerabilities that could impact the partnership's success.
- iii. Integrate BEN's AI technology into AFG's dealership systems and databases seamlessly and efficiently to ensure operational success.

35. During negotiations, AFG and Brewer made repeated assurances about AFG's operational capacity, dealership databases and data security compliance. These representations were material to BEN's decision to enter into the Reseller Agreement, as BEN sought to protect its proprietary technology and reputation from potential risks posed by AFG's systems and to integrate with AFG's databases.

36. AFG's CEO, Brewer, actively participated in the negotiation of the Reseller Agreement and personally guaranteed AFG's readiness to fulfill its data and access to pilot obligations. Brewer's assurances extended beyond AFG's general operational capacity, including

specific commitments regarding AFG's ability to handle sensitive dealership and consumer data securely.

37. Despite these representations, as detailed below, AFG was not operationally prepared, and its operational systems (the "P" database drive") were compromised by a ransomware attack just days before the execution of the Reseller Agreement. These facts were actively concealed by Brewer and AFG, constituting material misrepresentations and omissions that induced BEN into the agreement.

38. The Reseller Agreement was not merely a routine commercial transaction; it was a critical business initiative for BEN to establish a foothold in the automotive market. BEN relied on AFG and Brewer's representations as the foundation for its strategic expansion, believing the partnership would provide a secure and reliable channel to deploy its AI technology.

### **C. Brewer's Stock and Warrant Agreements**

39. As part of the Exclusive Reseller Agreement executed on August 19, 2023, Defendant Ralph Wright Brewer III negotiated substantial personal financial benefits tied to BEN's stock and warrants. These agreements were central to Brewer's motivation to induce BEN into entering the Exclusive Reseller Agreement through misrepresentations and omissions.

40. Specifically, BEN allocated 1.75 million shares of its stock to AFG in September 2023, subject to the completion of the merger, valued at \$10 per share at the time of issuance. Those shares were subsequently transferred in March of 2024 to AFG. This initial allotment provided AFG with stock valued at \$17.5 million. Shortly after BEN began publicly trading on or about March 15, 2024, BEN's stock price rose to \$19 per share, significantly increasing the value of AFG's holdings to approximately \$33.25 million, creating a personal financial windfall for Brewer and AFG.

41. In addition to the stock allotment, AFG also secured a warrant agreement as part of the Exclusive Reseller Agreement. This warrant agreement granted AFG the right to purchase an additional 1 million shares of BEN stock at \$10 per share, subject to performance benchmarks related to AFG's obligations and performance under the Exclusive Reseller Agreement. At the time the stock price reached \$19, this warrant provided Brewer with an unrealized potential profit of approximately \$9 million if exercised.

42. The stock and warrant agreements were predicated on the assumption that AFG, under Brewer's leadership, would fulfill its obligations under the Exclusive Reseller Agreement, including compliance with data security standards and successful integration of BEN's AI technology into AFG's databases and dealership systems. AFG's and Brewers significant financial stake in BEN's stock value and his personal gains from the warrant agreement tied him directly to the success of the partnership.

43. However, as detailed elsewhere in this complaint, Brewer's representations regarding AFG's readiness to perform under the Exclusive Reseller Agreement were false. At the time of the agreement's execution, AFG had recently suffered a ransomware/data breach attack that compromised customer social security numbers and over 105,000 sensitive files, rendering its systems inoperable. This attack, concealed by Brewer, directly impacted AFG's ability to meet its obligations and posed significant risks to BEN

44. Brewer's concealment of the ransomware attack and misrepresentations about AFG's compliance and technology readiness dealers' systems induced BEN into issuing the stock and warrants. Brewer's financial gains from these agreements were obtained through fraud and bad faith conduct, entitling BEN to seek rescission of the stock and warrant agreements and recover damages for the resulting harm.

45. Brewer's bad faith actions not only enriched him personally but also created conflicts of interest that undermined the entire partnership's success and loss of trust in Brewer/AFG. Despite having a direct financial incentive tied to BEN's stock price, Brewer failed to ensure that AFG fulfilled its obligations, instead engaging in retaliatory conduct when BEN raised concerns about AFG's noncompliance. Even worse, Brewer's scheme included taking his newly acquired ill-gotten gains in BEN stock to invest in Brewer's own competitor AI company against BEN.

**D. The Concealment of the Ransomware Attack on AFG Data Breach from BEN**

46. On August 13, 2023, just six days before BEN and AFG. AFG executed the Reseller Agreement, AFG's systems were crippled by a devastating ransomware attack perpetrated by the notorious "ALPHV" group, an affiliate of the BlackCat ransomware organization. This attack rendered AFG's systems inoperable and compromised over 105,000 files, including sensitive consumer and dealership data. In order to avoid payment of a ransom in the estimated range of 3 and 12 million dollars, Brewer refused to engage in any kind of communication with the threat actor.

47. The ransomware attack targeted AFG's central database of dealer systems, customer information, and IT infrastructure, encrypting files and locking out critical operational systems. The threat actor or/and hacker gained "root access" according to Amanda Tettleton, CFO of AFG. The attackers issued a demand for ransom, threatening to publish or destroy sensitive data if payment was not made. The compromised data obtained from AFG included financial records, dealership contracts, warranty files, and private consumer information, including social security numbers, creating an immediate and substantial risk of regulatory and legal exposure for AFG and soon to be unsuspecting business partner BEN.

48. AFG's executive leadership, including CEO Ralph Wright Brewer III, became aware of the attack immediately. However, instead of addressing the crisis honestly and transparently, Brewer and AFG leadership engaged in a deliberate campaign to destroy all evidence and conceal the breach. Brewer falsely portrayed the disruption as "routine system maintenance" in internal and external communications, including during ongoing negotiations with BEN. Brewer made no effort to notify BEN, the AFG dealership clients, or regulatory authorities about the attack, as required under both the Reseller Agreement and applicable data protection laws.

49. The ransomware attack occurred during a critical period in the negotiations between BEN and AFG. Brewer knew that disclosure of the attack would jeopardize AFG's ability to finalize the Reseller Agreement and the associated financial benefits, including stock and warrant agreements tied to AFG's performance. Brewer and AFG executives thus made a calculated decision to suppress this material information and proceed with the execution of the agreement under false pretenses.

50. Brewer and AFG also failed to take appropriate remedial measures to mitigate the consequences of the ransomware attack. Despite the severe compromise of its systems, AFG did not engage cybersecurity experts to address vulnerabilities, secure compromised data, or notify affected parties. Instead, Brewer prioritized concealing the breach to protect his personal financial interests and maintain the appearance of operational stability.

51. AFG Companies and CareGard Warranty Services had no Incident Response Plan ("IRP") in place to adequately respond to any cyber-attack. As required by various laws and regulations, including the Federal Trade Commission, Gramm-Leach-Bliley Act ("GLBA") and FTC Safeguard, AFG had a duty to protect its investors, stockholders, and most importantly its

consumers and customers. Despite full knowledge of the cyberattack, AFG and Brewer failed to file data breach notifications with approximately forty-eight states and other Federal Agencies, including the Federal Trade Commission under the GLBA and the updated Federal Trade Commission Safeguards Rule.

52. It became clear, through Brewer's inaction and refusal, that Brewer and AFG's intention was to conceal, secret and hide the event to remain noncompliant and ensure business negotiations would not be harmed.

53. On or about March 21, 2024, Travis Gates, former president of AFG Technologies notified the Office of the Attorney General of the State of Maryland of AFG's failure to file data breach notifications within the state.

54. On or about March 23, 2024, a separate individual notified the Office of the Attorney General of the State of California of AFG's failure to file data breach notifications within the state.

55. On April 22, 2024, Automotive News published an article under its finance and insurance section outlining a data breach event within CareGard. A true and correct copy of the Automotive News Article is attached hereto as **Exhibit C**.

56. The concealment of the ransomware attack constituted a **material omission** that directly induced BEN to finalize the Exclusive Reseller Agreement. Had BEN been aware of the attack, it would not have entered into the agreement or issued stock and warrants to Brewer and AFG. The concealed breach created immediate risks to BEN's proprietary technology, reputation, and regulatory compliance, which were only discovered after the agreement was executed.

57. The ransomware attack not only violated the Exclusive Reseller Agreement's disclosure requirements but also breached state and federal data protection laws, including the

Gramm-Leach-Bliley Act (GLBA) and related Federal Trade Commission (FTC) Safeguards Rule. AFG's failure to disclose the attack exposed BEN to significant regulatory scrutiny and potential liability.

58. Brewer's decision to conceal the attack was part of a broader pattern of bad faith conduct aimed at enriching himself personally at the expense of BEN. Brewer's actions and omissions during and after the ransomware attack created long-term consequences for BEN, including damage to its reputation, lost business opportunities, and the need to invest significant resources into mitigating risks associated with the compromised partnership.

**E. March 7, 2024, AFG "Vision Meeting"**

59. On March 7, 2024, AFG held its "Vision Meeting" to set its five-year plan to set up its own AI company, Pathwai, to compete against BEN in the automotive AI marketplace. Ralph Wright Brewer, Chief Executive Officer of AFG, Jason DeLaporte (President of Pathwai Inc), William "Bill" Bigley (Chief Financial Officer of AFG), Amanda Tettleton (Chief Accounting Officer of AFG), Keith Cooper (Chief Operations Officer of AFG), Dave Duggan (Chief Technology Officer of AFG), Travis Gates (Former Chief Compliance Officer of AFG) and Erick Roberts (Former Vice President of Software of AFG) were all in attendance.

60. According to witnesses at the meeting on March 7, 2024, AFG's President, Jason De Laporte, stated that AFG "did not have the operational capacity to fulfill the exclusive reseller agreement" with BEN and also planned to violate the exclusivity clauses within the exclusive reseller agreement. De Laporte continued on, stating, *"If we do the SET deal, because now I don't have to go to market, I don't have to sell, I don't have to do all these things."*

61. BEN was never informed of other material information regarding AFG's intent to violate the exclusive reseller agreement. For example, BEN was not told about AFG's relationship



with another test dealership or AFG's intent not to meet its contractual requirements related to BEN's AI software.

62. According to witnesses present at the meeting, Dave Duggan stated: "if the technology were developed now and ready to go, they would all be signing up . . . We might be able to accelerate this actually because the technician assistant, BEN AI can do most of that without a ton of development on our side, because its feeding manuals." As such, not only could AFG not fulfill its commitment to BEN, but it was also wholly unprepared to move forward with any agreements.

63. Also, according to witnesses present at the March 7<sup>th</sup> meeting, Brewer blatantly admitted his intention to violate the exclusivity and non-compete provisions of the exclusive reseller agreement with BEN even before receiving BEN stock. Specifically, Wright Brewer stated, "to be quite frank with, the person we have to compete against (BEN), potentially on those ten companies, would be BEN Inc." Brewer exclaimed to the AFG team, "Oh no we keep everything," which was Brewer's strategy all along to compete against BEN, and to never provide BEN with any automotive dealer systems information for BEN AI Automotive.

64. AFG executives also outwardly acknowledged during this meeting that the ransomware attack and data breach in August of 2023 were concealed from BEN so AFG could fraudulently obtain BEN stock grants. Keith Cooper stated, "we're just lucky" that SET hasn't asked for any kind of notification since the data breach. As Travis Gates reminded the group, "the real concern is" that SET is going to ask for details of the ransomware attack, and "we're already in violation of our agreement" with regards to cyber security industry standards and the FTC Safe Guard guidelines.

65. At the March 7<sup>th</sup> meeting, Dave Duggan acknowledged that AFG was still behind in meeting AFG's cyber security industry standards and regulatory compliance. Dugan stated, "I'm sorry, I'm looking at accelerate completion of SOC2 and FTC Safeguards compliance."

66. Finally, at the March 7<sup>th</sup> meeting, Brewer acknowledged that even eight months later, AFG still had no database or dealer systems information to launch any products for AFG, let alone data sets for BEN under AFG's contractual obligations. Brewer made is clear the utter lack of functional data systems at AFG by stating, "so knowing the type of reports that their looking for, and knowing when we can put our database, finish our database with all the CareGard data, what does that look like" and "that depends on when the database is going to be completed."

#### **F. Material Misrepresentations and Omissions**

67. In June 2023, BEN and DHC Acquisition, Corp. ("DHCA"), a blank check company incorporated as a Cayman Islands exempted company for purpose of entering into a merger. BEN and DHCA had a non-binding letter of intent to acquire AFG for \$120 million. This occurred just prior to the ransomware attack, and this deal later changed to the exclusive reseller agreement with BEN as AFG did not have the required audited financials needed to close. AFG subsequently agreed to a financing commitment when the business combination was consummated.

68. The business combination agreement, dated September 7, 2023, involved the merger between the prior BEN and DHCA.

69. During negotiations for the Exclusive Reseller Agreement, AFG and its CEO, Ralph Wright Brewer III, repeatedly assured BEN that AFG's systems were fully operational, compliant with data security standards, and capable of integrating BEN's AI-powered customer

engagement solutions. These assurances were a critical factor in BEN's decision to enter into the Exclusive Reseller Agreement.

70. Brewer specifically represented that AFG had robust data security protocols in place and that its IT infrastructure was fully prepared to support BEN's proprietary technology. Brewer emphasized AFG's long-standing reputation in the automotive industry, presenting AFG as a reliable and trustworthy partner.

71. AFG has provided significant financing for BEN. For example, in its S-1 filing, BEN described its interim financing as follows:

#### Interim Financings

On September 29, 2023, AFG Companies Inc. ("AFG") purchased 456,621 shares of Common Stock for \$2.19 per share for an aggregate purchase price of approximately \$1.0 million (the "AFG Interim Financing") and, in accordance with the terms thereof, AFG's obligation to purchase shares of Common Stock immediately prior to the Effective Time (as defined in the Subscription Agreement described below) under the Subscription Agreement was reduced by \$1.0 million. . . . BEN expects to use the proceeds of the Interim Financings for working capital and expenses related to the Business Combination (as defined below).

BEN's revenue growth is also dependent on AFG as its exclusive reseller. According to

BEN's filings:

Our revenue growth depends in part on the success of our strategic relationships with third parties, including channel partners, and if we are unable to establish and maintain successful relationships with them, our business, operating results, and financial condition could be adversely affected.

We rely, in part, on channel providers as a way to grow our business and customer bases. We anticipate that we will continue to establish and maintain relationships with third parties, such as channel partners, resellers, OEMs, system integrators, independent software and hardware vendors, and platform and cloud service providers. For example, in August 2023, we entered into a Reseller Agreement (as defined below) with AFG Companies Inc. ("AFG") whereby AFG operates as the exclusive channel partner and

reseller of certain of our projects in the motor vehicle marketing and manufacturing industry for a term of five years (emphasis added).

72. Despite representations, Brewer and AFG concealed the August 13, 2023, ransomware attack, which compromised all files, including over 105,000 encrypted files and rendered AFG's systems inoperable. Brewer knew that disclosing the attack would jeopardize the partnership and his personal financial gains tied to BEN's stock and warrants.

73. While BEN disclosed to its investors AFG's importance to the company's financing, revenue growth, and technology (one that aims to maintain "**compliance with applicable privacy and data protection laws and regulations**"), it omitted material facts regarding AFG's ransomware attack, data breach, and lack of adequate cybersecurity policies due to omission made by AFG. This is in direct violation of the SEC's requirements regarding disclosing material cybersecurity incidents. Specifically, under Item 1.05 of Form 8-K, public companies must disclose information about material cybersecurity incidents within four business days after the company determines that a cybersecurity incident is material. A material incident is one that a reasonable investor would consider important in making an investment decision.

74. By concealing the attack, Brewer and AFG falsely created the impression that AFG was capable of meeting its obligations under the Reseller Agreement, including the integration of BEN's AI technology into dealership systems. In reality, AFG's systems were crippled, and its ability to perform under the agreement was severely impaired.

75. Brewer and AFG also failed to disclose their non-compliance with federal and state data protection laws, including the Gramm-Leach-Bliley Act (GLBA) and the Federal Trade Commission's Safeguards Rule. AFG lacked an incident response plan and failed to implement adequate cybersecurity measures, leaving its systems vulnerable to attacks like the one it experienced.

76. These omissions were material to BEN's decision to enter the Exclusive Reseller Agreement, as BEN relied on AFG's assurances of compliance to protect its proprietary technology and reputation.

77. Brewer and AFG also made false and misleading statements about AFG's financial stability and performance during the negotiations. Brewer presented AFG as a financially sound company with a proven track record of successful partnerships in the automotive industry. However, Brewer failed to disclose financial challenges faced by AFG, including liabilities arising from the ransomware attack and operational disruptions caused by the compromised systems.

78. Brewer's misrepresentations created the illusion that AFG was a stable and capable partner, inducing BEN to issue stock and warrants valued at millions of dollars.

79. Brewer and AFG's material misrepresentations and omissions directly induced BEN to execute the Reseller Agreement and issue valuable stock and warrants to Brewer and the AFG entities. BEN relied on the false representations about AFG's operational readiness, data security compliance, and financial stability in making these decisions.

80. As a result of these misrepresentations, BEN suffered significant harm, including:

- i. Exposure to regulatory scrutiny and liability due to AFG's non-compliance with data protection laws.
- ii. Damage to its reputation and loss of trust among business partners and clients.
- iii. Financial losses stemming from the diminished value of the Reseller Agreement and the costs of mitigating risks associated with the compromised partnership.

81. Brewer personally participated in and directed the misrepresentations and omissions described above. As CEO of AFG, Brewer had knowledge of the ransomware attack, AFG's non-compliance with data security standards, and the company's financial challenges.

Brewer intentionally withheld this information from BEN to secure personal financial benefits tied to the Reseller Agreement, including stock and warrants valued at millions of dollars.

82. Brewer's actions demonstrate a pattern of bad faith and fraudulent intent, further justifying BEN's claims for rescission of the agreement, damages, and other relief.

**G. AFG Breach of the Due Figlie Consulting Agreements**

83. On March 1, 2022, Due Figlie entered into a Consulting Agreement with AFG represented by its CEO, Ralph Wright Brewer III. A true and correct copy of the March 1, 2022, Agreement is attached hereto as **Exhibit D**. Under this agreement, Due Figlie provided consulting services to AFG and played a significant role in generating new business for CareGard Warranty Services, Inc., one of AFG's affiliated entities.

84. The March 2022 agreement required AFG to:

- i. Pay an Agent Fee of up to \$1.00 per contract for all new business brought to CareGard Warranty Services through Due Figlie's efforts.
- ii. Negotiate in good faith the allocation of founder shares in Tronix, an affiliated business.
- iii. Provide milestone equity compensation of up to 20% ownership in Tronix, contingent upon performance benchmarks achieved through Due Figlie's contributions.

85. On June 1, 2022, the Consulting Agreement was updated to reiterate the terms of the March 2022 agreement. A true and correct copy of the June 1, 2022, Agreement is attached hereto as **Exhibit E**. This included a reaffirmation of Due Figlie's entitlement to:

- i. Agent Fees tied to new business generated for CareGard Warranty Services.
- ii. Equity compensation and founder shares based on its significant contributions to Tronix.
- iii. The updated agreement reflected Due Figlie's ongoing role in driving business growth and expanding AFG's market presence.

86. Due Figlie fully performed its obligations under both Consulting Agreements, generating substantial new business for CareGard Warranty Services and significantly enhancing the financial position of AFG and its affiliates.

87. Through its efforts, Due Figlie established new client relationships, increased contract volumes, and contributed to the overall profitability of AFG's operations. These contributions directly benefited Brewer and the AFG entities, aligning with the agreed-upon performance benchmarks.

88. Despite Due Figlie's full performance, Brewer, acting on behalf of AFG, repudiated the Consulting Agreements in a July 18, 2023, email to Shawn Lucas. In this email, Brewer dismissed the agreements as "new company-crap" and denied any obligation to honor the terms of the agreements.

89. Brewer further stated that he did not sign the August 2022 update to the Consulting Agreements and refused to negotiate milestone equity compensation or provide the founder shares Due Figlie was entitled to under the agreements.

90. In the same July 2023 email, Brewer demanded that Due Figlie provide a release absolving him and AFG of all obligations related to the Consulting Agreements and Tronix. Brewer threatened to "escalate the situation" and end all negotiations if the release was not delivered.

91. Brewer's statements and actions were part of a broader pattern of bad faith conduct aimed at evading AFG's contractual obligations and denying Due Figlie the compensation it was owed.

92. Brewer's repudiation of the Consulting Agreements caused significant harm to Due Figlie, including:

- i. The loss of Agent Fees tied to new business generated for CareGard Warranty Services.
- ii. The denial of founder shares and milestone equity compensation, which were key elements of the agreements.
- iii. Reputational harm and lost opportunities arising from Brewer's bad faith conduct and refusal to honor AFG's contractual obligations.
- iv. Due Figlie's contributions to AFG and its affiliates were instrumental in their financial success, yet Brewer and AFG sought to avoid compensating Due Figlie for its efforts.

93. Brewer's repudiation of the Consulting Agreements was not an isolated incident but part of a deliberate strategy to enrich himself at the expense of Due Figlie. Brewer personally directed AFG's refusal to honor the agreements and leveraged his control over the AFG entities to deny Due Figlie its rightful compensation.

94. Brewer's actions demonstrate bad faith and a disregard for contractual obligations, further justifying the claims for damages, rescission, and other relief sought by Due Figlie and BEN.

#### **H. Brewer's Retaliation and Bad Faith Conduct**

95. Following BEN's discovery of AFG's failure to comply with its obligations under the Reseller Agreement, including the concealment of the ransomware attack and the inability to meet performance benchmarks, BEN sought to address these issues collaboratively.

96. Instead of engaging in good faith to resolve these concerns, Brewer responded with open hostility toward BEN and its leadership. Brewer began making statements and taking actions aimed at undermining BEN's business interests and avoiding accountability for AFG's breaches and misconduct.

97. Unbeknown to BEN, in October 2023, Brewer explicitly declared in an internal meeting with executive leadership of AFG that AFG was, "going to war" and "had to own all of this" (referring to the intellectual property of BEN). This statement reflected Brewer's intent to



retaliate against BEN rather than work toward a resolution. AFG continued to demand access to BEN's source code.

98. Brewer's declaration of war was not an idle threat. It was followed by a series of deliberate actions aimed at damaging BEN, including:

- i. Failing to perform under the Reseller Agreement while retaining the financial benefits provided by BEN, such as the stock and warrants issued to Brewer and AFG.
- ii. Refusing to cooperate with BEN to address the risks posed by the ransomware attack and mitigate the resulting harm.
- iii. Disparaging BEN to third parties in an effort to harm its reputation and business relationships.

99. Brewer's hostility was not limited to BEN but also extended to Due Figlie, which had raised concerns about AFG's failure to honor its obligations under the Consulting Agreements. Brewer's July 18, 2023, email to Shawn Lucas demonstrated his intent to repudiate the agreements and avoid compensating Due Figlie for its substantial contributions to AFG's success.

100. Brewer threatened to escalate the situation and end all negotiations with BEN unless it provided a release absolving Brewer and AFG of their contractual obligations with respect to Due Figlie. These threats were part of Brewer's broader strategy to avoid accountability for his actions while continuing to benefit from Due Figlie's performance under the agreements.

101. Brewer's actions reflect a consistent pattern of bad faith conduct aimed at enriching himself at the expense of BEN and Due Figlie. This pattern includes:

- i. Concealing material facts during the negotiation of the Reseller Agreement, including the ransomware attack and AFG's non-compliance with data security standards.
- ii. Retaining financial benefits tied to BEN's stock and warrants while failing to ensure AFG's performance under the Reseller Agreement.
- iii. Repudiating the Consulting Agreements with Due Figlie and denying its rightful compensation.

- iv. Threatening and retaliating against BEN and Due Figlie to avoid accountability for his and AFG's breaches.

102. Brewer's retaliation and bad faith conduct caused significant harm to BEN and Due Figlie, including:

- i. Financial losses resulting from AFG's failure to perform under the Reseller Agreement.
- ii. Damage to BEN's reputation and business relationships due to Brewer's disparaging statements and failure to address the ransomware attack.
- iii. Loss of Agent Fees, equity compensation, and founder shares owed to Due Figlie under the Consulting Agreements.
- iv. Brewer's actions have not only undermined the partnerships and agreements at issue but also demonstrated his intent to avoid accountability while personally benefitting from the financial gains tied to BEN's stock and warrants.

103. Brewer's retaliatory conduct and bad faith actions form a critical part of the claims in this lawsuit. His statements and behavior demonstrate a deliberate strategy to evade obligations, harm BEN and Due Figlie, and prioritize his personal financial interests over the success of the partnerships and agreements.

#### **I. AFG/Brewer Causes Financial Losses to BEN**

104. As a direct result of the Defendants' breaches of contract, material misrepresentations, omissions, and bad faith conduct, BEN has suffered significant financial harm. These damages include:

- i. Loss of anticipated revenue from the Reseller Agreement due to AFG's failure to perform its obligations, including the inability to successfully integrate BEN's AI-powered technology into dealership systems.
- ii. Costs incurred by BEN to address and mitigate risks arising from AFG's concealed ransomware attack, including regulatory compliance efforts, IT security upgrades, and reputational repair initiatives.

- iii. Losses tied to the issuance of stock and warrants to Brewer and AFG, which were based on fraudulent representations about AFG's compliance, readiness, and operational capacity.

105. The concealment of the ransomware attack and AFG's subsequent non-performance under the Reseller Agreement damaged BEN's reputation in the automotive industry. As an innovator in the AI-powered solutions, BEN relies on its reputation for technological excellence and data security to build partnerships and secure business opportunities.

106. AFG's retaliatory statements and disparagement of BEN to third parties further eroded trust and confidence in BEN's brand, harming its ability to maintain existing business relationships and develop new partnerships.

107. AFG's failure to comply with data security standards and its concealment of the ransomware attack created significant regulatory and legal risks for BEN. These include:

- i. Potential liability under state and federal data protection laws, including the Gramm-Leach-Bliley Act (GLBA) and Federal Trade Commission (FTC) Safeguards Rule.
- ii. Investigations and scrutiny from regulatory authorities regarding BEN's role in the partnership with AFG and its failure to detect or disclose the concealed attack.
- iii. Costs associated with defending against potential lawsuits from affected third parties, such as dealerships and consumers whose data was compromised during the ransomware attack.

108. The failure of the Reseller Agreement undermined BEN's strategic efforts to expand into the automotive market. This partnership was intended to establish a foothold in a competitive industry, leveraging AFG's existing relationships to deploy BEN's AI technology at scale.

109. By entering into a partnership based on fraudulent misrepresentations, BEN was deprived of the opportunity to pursue alternative, legitimate partnerships that could have achieved these strategic objectives.

110. Defendants' repudiation of the Consulting Agreements caused significant harm to Due Figlie, which fully performed its obligations and provided substantial value to AFG and its affiliates. These damages include:

- i. Loss of Agent Fees tied to new business generated for CareGard Warranty Services, which constituted a critical source of revenue for Due Figlie under the agreements.
- ii. Denial of founder shares and milestone equity compensation owed to Due Figlie based on its contributions to Tronix development and success.
- iii. Reputational harm and lost business opportunities arising from Brewer's bad faith conduct and refusal to honor AFG's contractual obligations.

111. The interconnected nature of the Exclusive Reseller Agreement and Consulting Agreements amplified the harm caused by Brewer's and AFG's misconduct. Due Figlie's performance under the Consulting Agreements contributed directly to AFG's financial success, which was essential to the success of the Reseller Agreement with BEN

112. By repudiating the Consulting Agreements and failing to perform under the Reseller Agreement, Brewer and AFG created cascading effects that undermined both partnerships, causing significant harm to BEN and Due Figlie alike.

113. The harm caused by Brewer, AFG, and the affiliated entities extends beyond financial losses to include reputational damage, regulatory exposure, and lost opportunities for both BEN and Due Figlie. These damages are the direct result of Defendants' fraudulent conduct, material omissions, and bad faith actions, and they form the basis for the relief sought in this lawsuit.

## **J. Defendants' Misconduct**

114. Defendant Ralph Wright Brewer III orchestrated and directed the misconduct detailed in this lawsuit. As CEO AFG and its affiliated entities, Brewer exercised complete control over the companies, using them as his personal tools to defraud BEN and Due Figlie.

115. Brewer's actions were not isolated incidents but part of a deliberate scheme to enrich himself at the expense of BEN and Due Figlie. By concealing material facts, misrepresenting AFG's compliance and capabilities, and repudiating contractual obligations, Brewer acted in bad faith and violated the trust placed in him by the parties he partnered with.

116. The AFG entities—Automotive Financial Group, Inc., AFG Companies, Inc., AFG Technologies, LLC, CareGard Warranty Services, Inc., Southwest Colonial Reinsurance, Ltd., and Prime Reserve Plus, Inc. DaidaX, Inc. f/k/a Pathwai Inc. and BEN Automotive Inc.—were integral to the fraudulent schemes carried out by Brewer.

117. These entities participated in and benefited from Brewer's fraudulent representations and omissions, including:

- i. The concealment of the August 13, 2023, ransomware attack that compromised sensitive consumer and dealership data.
- ii. The misrepresentation of AFG's compliance with data security standards during negotiations with BEN
- iii. The repudiation of the Consulting Agreements with Due Figlie, depriving it of rightful compensation for its substantial contributions.

118. Brewer and the AFG entities pursued a coordinated strategy of concealment and retaliation to avoid accountability and maximize their financial gains. This strategy included:

- i. Concealing the ransomware attack from BEN and failing to disclose material risks that undermined the Reseller Agreement.
- ii. Misleading BEN about AFG's operational readiness and compliance, inducing BEN to issue stock and warrants tied to AFG's performance.

- iii. Retaliating against BEN and Due Figlie when they attempted to enforce their contractual rights, including Brewer's explicit declaration, "We're going to war."

119. The actions of Brewer and the AFG entities caused significant harm to both BEN and Due Figlie. These damages, as outlined earlier, include:

- i. Financial losses tied to AFG's failure to perform under the Reseller Agreement.
- ii. Damage to BEN's reputation and regulatory exposure due to AFG's non-compliance with data security laws.
- iii. Loss of Agent Fees, founder shares, and milestone equity compensation owed to Due Figlie under the Consulting Agreements.

**K. Piercing the Corporate Veil – Brewer's Misuse of the AFG Entities**

120. Brewer's misuse of the AFG entities demonstrates a clear need to pierce the corporate veil and hold him personally liable. Brewer disregarded corporate formalities, undercapitalized the AFG entities, and used them as his alter ego to carry out fraudulent and retaliatory actions.

121. Brewer's actions show a consistent pattern of personal enrichment and bad faith conduct, which cannot be shielded by the corporate entities he controlled. Holding Brewer personally liable is essential to ensure accountability for the harm caused to BEN and Due Figlie.

122. The harm caused by Brewer and the AFG entities continues to affect BEN and Due Figlie, requiring significant resources to address and mitigate. Both BEN and Due Figlie have suffered long-term financial and reputational damage, limiting their ability to pursue business opportunities and maintain trust with partners and clients.

123. This lawsuit seeks to hold Brewer and the AFG entities accountable for their actions and secure the relief necessary to compensate BEN and Due Figlie for the harm they have suffered.

#### IV. CAUSES OF ACTION

##### COUNT 1

##### Breach of Contract

**(Against Automotive Financial Group, Inc., AFG Companies, Inc., and CareGard Warranty Services, Inc.)**

124. Plaintiff realleges each and every allegation set forth above and incorporates them herein.

125. To establish a breach of contract claim under Texas law, the Plaintiff must prove 1) the existence of a valid contract; 2) Plaintiff's performance or tendered performance; 3) Defendants breach of the contract; and 4) damages sustained as a result of the breach.

126. On August 19, 2023, BEN entered into a valid and enforceable Reseller Agreement with Defendant AFG. Under the terms of the Reseller Agreement, AFG agreed to, among other things: Maintain strict compliance with data security standards and all applicable state and federal laws; disclose any cybersecurity incidents or vulnerabilities that could affect the partnership; and successfully integrate BEN's proprietary AI technology into its dealership systems.

127. This agreement was supported by mutual consideration: BEN provided its AI-powered customer engagement technology, while AFG gained exclusive rights to resell this technology within the automotive industry.

128. Plaintiff BEN fully performed its obligations under the Reseller Agreement, including delivering its proprietary AI technology to AFG, relying on AFG's representations of operational readiness and compliance with data security standards, and collaborating with AFG to integrate the technology into dealership systems.

129. BEN acted in good faith throughout the partnership, fulfilling all conditions precedent and cooperating with AFG to implement the Reseller Agreement.

130. AFG materially breached the Reseller Agreement in multiple ways. On August 13, 2023, six days before executing the Reseller Agreement, AFG suffered a devastating ransomware attack that compromised over 105,000 sensitive files and rendered its systems inoperable. AFG failed to disclose this critical incident to BEN, violating the contractual requirement to disclose cybersecurity vulnerabilities.

131. AFG misrepresented its compliance with applicable data protection laws, including the GLBA the FTC Safeguards Rule. AFG lacked an incident response plan and failed to secure its IT infrastructure, breaching the express terms of the Reseller Agreement.

132. AFG failed to integrate BEN's AI technology into its dealership systems, which was a central purpose of the agreement. This failure stemmed from AFG's inability to operate effectively after the ransomware attack, which it had actively concealed.

133. AFG's breaches were willful and deliberate, as evidenced by CEO Ralph Wright Brewer III's active concealment of the ransomware attack and misrepresentation of AFG's operational readiness.

134. As a direct and proximate result of AFG's breaches, Plaintiff BEN suffered substantial financial and reputational harm.

135. The Reseller Agreement was a cornerstone of BEN's strategic expansion into the automotive market, and AFG's breaches undermined this critical business initiative. AFG's actions—or lack thereof—were not only material breaches but were also compounded by bad faith conduct, including the concealment of material facts and misrepresentations made during the negotiation of the agreement.



**COUNT 2**

**Fraud**

**(Against Ralph Wright Brewer III and All AFG Entities)**

136. Plaintiff re-alleges and incorporates by reference each and every allegation set forth above.

137. To establish a claim for fraud under Texas law, Plaintiff must prove that Defendants made a material representation that was false, knew it was false or made it recklessly without knowledge of its truth, intended for Plaintiff to rely on the representation, and caused Plaintiff harm when it did so. Each element is satisfied here.

138. Defendants, led by Ralph Wright Brewer III, made numerous material misrepresentations during negotiations and the execution of the Reseller Agreement. Specifically, Brewer and AFG represented that AFG was fully operational, compliant with applicable data security standards, and capable of successfully integrating BEN's proprietary AI technology into its dealership systems. Brewer assured BEN that AFG had robust cybersecurity protocols in place and that no incidents or vulnerabilities existed that could jeopardize the partnership. These representations were critical to BEN's decision to execute the Reseller Agreement, issue stock and warrants to Brewer, and move forward with the strategic partnership.

139. These representations were knowingly false. Just six days before executing the Reseller Agreement, AFG suffered a crippling ransomware attack on August 13, 2023, which rendered its systems inoperable and compromised over 105,000 sensitive files, including financial records and consumer data. Brewer, fully aware of the attack, deliberately concealed this material information from BEN Rather than disclose the attack as required under the Reseller Agreement and applicable law, Brewer falsely portrayed the system disruptions as routine maintenance. AFG

was also in violation of multiple data protection laws, including the Gramm-Leach-Bliley Act (GLBA) and the FTC Safeguards Rule, as it lacked an incident response plan and adequate cybersecurity protocols. AFG's operational capabilities were similarly overstated, as its compromised systems were entirely unprepared to support the integration of BEN's AI technology.

140. Brewer and AFG not only knew these representations were false but made them with the intent to induce BEN to rely on them. Brewer sought to secure significant personal financial benefits, including the issuance of 1.75 million shares of BEN stock and warrants for an additional 1 million shares. These financial arrangements were valued at millions of dollars and were tied directly to AFG's performance under the Reseller Agreement. Brewer and AFG also had a strong interest in finalizing the Reseller Agreement to maintain the appearance of stability and operational readiness while concealing the devastating impact of the ransomware attack.

141. Plaintiff BEN reasonably relied on Defendants' representations. Brewer's assurances regarding AFG's compliance and operational capabilities directly influenced BEN's decision to execute the Reseller Agreement and issue valuable stock and warrants. Brewer's position as CEO of AFG and his repeated assurances during negotiations gave BEN ample reason to trust the accuracy of his statements. Based on these representations, BEN entered into a partnership it believed would serve as the foundation of its expansion into the automotive industry, with AFG acting as a reliable and secure channel partner.

142. As a direct result of its reliance on these fraudulent representations, BEN suffered significant harm. BEN issued stock and warrants valued at millions of dollars to Brewer and AFG under false pretenses. AFG's inability to perform under the Reseller Agreement deprived BEN of anticipated revenue and strategic opportunities, while Brewer's concealment of the ransomware attack exposed BEN to regulatory scrutiny and reputational damage. BEN also incurred substantial

costs to mitigate the risks associated with AFG's breaches, including expenses for IT security upgrades, regulatory compliance efforts, and reputational repair.

**COUNT 3**

**Fraudulent Inducement**

**(Against Ralph Wright Brewer III and All AFG Entities)**

143. Plaintiff re-alleges and incorporates by reference each and every allegation set forth above.

144. Under Texas law, fraudulent inducement requires proof that a party made a material false representation, knew the representation was false, intended the other party to rely on it, and caused the other party to enter into an agreement that resulted in harm. The facts of this case establish each element of fraudulent inducement.

145. Defendants, led by Ralph Wright Brewer III, made deliberate and material misrepresentations to induce BEN into entering the Reseller Agreement. Brewer specifically represented that AFG was operationally ready and fully compliant with all data security standards. Brewer assured BEN that AFG had robust cybersecurity measures in place, was capable of securely handling sensitive dealership and consumer data and could seamlessly integrate BEN's AI-powered technology into its dealership systems. These representations were critical because BEN relied on them to protect its proprietary technology and its reputation in the automotive industry. Brewer further assured BEN that no cybersecurity incidents or vulnerabilities could interfere with the success of the partnership.

146. These representations, however, were patently false and knowingly so. Just six days before the execution of the Reseller Agreement, AFG suffered a catastrophic ransomware attack that rendered its systems inoperable and compromised over 105,000 files containing sensitive

financial, dealership, and consumer data. Brewer was fully aware of this attack and its implications. Rather than disclose the incident, Brewer and AFG actively concealed it and falsely portrayed the resulting disruptions as routine system maintenance. At the time of the Reseller Agreement, AFG's systems were severely compromised, and the company was incapable of meeting its obligations. Brewer further misrepresented AFG's compliance with federal and state data protection laws, despite knowing that AFG lacked adequate cybersecurity protocols, an incident response plan, or the operational capacity to fulfill its contractual obligations.

147. Brewer made these misrepresentations with the specific intent to induce BEN into entering the Reseller Agreement. Securing the agreement was essential to AFG's financial survival and Brewer's personal financial gain. As part of the agreement, Brewer negotiated for himself a substantial personal benefit in the form of 1.75 million shares of BEN stock, valued at \$17.5 million at the time of issuance, and [warrants for an additional 1 million shares]. Brewer knew that disclosure of the ransomware attack or AFG's operational deficiencies would jeopardize the deal and his financial windfall. By concealing these facts, Brewer ensured that BEN would execute the agreement under false pretenses.

148. BEN reasonably relied on Brewer's representations in deciding to enter the Reseller Agreement. Brewer, as the CEO of AFG, was in a position of authority and trust, and BEN had no reason to doubt his assurances regarding AFG's operational readiness and compliance with data security standards. These assurances were material to BEN's decision to enter into the agreement and issue millions of dollars' worth of stock and warrants to Brewer and AFG. BEN justifiably believed that AFG was capable of fulfilling its obligations and that the partnership would be a cornerstone of its expansion into the automotive sector.

149. As a direct result of this fraudulent inducement, BEN suffered significant harm. AFG's inability to perform under the Reseller Agreement deprived BEN of the anticipated revenue and strategic benefits of the partnership. The concealment of the ransomware attack exposed BEN to regulatory scrutiny, reputational damage, and substantial costs to address the risks associated with AFG's breaches. Additionally, BEN issued stock and warrants to Brewer and AFG, valued at over \$33.25 million, based on fraudulent misrepresentations. These financial and reputational damages were foreseeable and directly caused by Brewer's deliberate and deceptive conduct.

150. Brewer's actions were intentional, calculated, and egregious. His fraudulent inducement was designed to enrich himself and his affiliated entities at BEN's expense, while deliberately concealing material facts that would have prevented the execution of the Reseller Agreement. As a result, BEN was irreparably harmed, both financially and reputationally.

#### **COUNT 4**

#### **Securities Fraud**

#### **(Against Ralph Wright Brewer III and Automotive Financial Companies, Inc.)**

151. Plaintiff re-alleges and incorporates by reference each and every allegation set forth above.

152. Securities fraud under Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 requires proof that a party made a material misrepresentation or omission in connection with the purchase or sale of securities, acted with scienter, and caused reliance and damages to the plaintiff. The facts here demonstrate that Defendants engaged in securities fraud by intentionally misrepresenting material facts and concealing critical information to secure the issuance of stock and warrants from BEN

153. In connection with the Reseller Agreement executed on August 19, 2023, Defendant Ralph Wright Brewer III negotiated substantial personal financial benefits tied to BEN's stock and warrants. Brewer received 1.75 million shares of BEN stock, valued at \$10 per share at the time of issuance, totaling \$17.5 million. Brewer also obtained a warrant to purchase an additional 1 million shares of BEN stock at \$10 per share, contingent upon certain performance benchmarks under the Reseller Agreement. The merger between DHCA and BEN was successful and shortly after the stock began trading on the NASDAQ under the stock symbol BNAI, BEN's stock price rose to \$19 per share, increasing Brewer's unrealized profits to over \$33.25 million. These financial benefits were directly tied to Brewer's misrepresentations and omissions.

154. Brewer, acting individually and on behalf of AFG, made deliberate and material misrepresentations to induce BEN to issue these securities. Brewer assured BEN that AFG was operationally ready, compliant with all applicable data security laws, and capable of meeting its obligations under the Reseller Agreement. These assurances included specific representations regarding AFG's ability to securely integrate BEN's proprietary AI technology into dealership systems. Brewer also omitted to disclose critical facts, including that just six days before executing the Reseller Agreement, AFG had suffered a devastating ransomware attack that rendered its systems inoperable and compromised over 105,000 files. Brewer's concealment of the ransomware attack and AFG's non-compliance with federal data protection laws were intentional omissions that materially affected BEN's decision-making.

155. Brewer and AFG acted with scienter, knowing that their representations and omissions were false or misleading. Brewer was fully aware of the ransomware attack and its impact on AFG's ability to meet its obligations. Rather than disclose the attack, Brewer intentionally concealed it and falsely assured BEN of AFG's operational readiness and compliance.

Brewer's conduct was not accidental or negligent but part of a calculated scheme to secure substantial personal financial benefits tied to BEN's stock and warrants. His actions demonstrate a willful disregard for the truth and a deliberate effort to mislead BEN

156. These material misrepresentations and omissions were made in connection with the purchase and sale of securities. Brewer's receipt of stock and warrants was a central component of the Reseller Agreement, and his fraudulent conduct directly influenced BEN's decision to issue these securities. The stock and warrants were issued based on the belief that AFG would perform under the Reseller Agreement and generate substantial revenue for BEN. Brewer's fraudulent inducement undermined the value of the partnership and the securities tied to it.

157. BEN justifiably relied on Brewer's misrepresentations and omissions in deciding to issue the stock and warrants. Brewer held a position of trust as the CEO of AFG, and his repeated assurances gave BEN no reason to doubt his claims. BEN reasonably believed that AFG was a reliable partner capable of fulfilling its obligations under the Reseller Agreement. Brewer's deliberate concealment of the ransomware attack and other material facts deprived BEN of the opportunity to make an informed decision.

158. As a direct result of Brewer's securities fraud, BEN suffered significant damages. The stock and warrants issued to Brewer and AFG were valued at over \$33.25 million, representing a substantial financial loss to BEN given AFG's inability to perform under the Reseller Agreement. BEN also incurred additional costs to mitigate the risks associated with AFG's failures, including regulatory compliance efforts, IT security upgrades, and reputational repair. The fraudulent issuance of securities caused both financial harm and reputational damage to BEN, further undermining its strategic objectives.

159. Brewer's conduct constitutes a clear violation of federal securities laws, including Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5. His actions were intentional, egregious, and designed to enrich himself at BEN's expense. Accordingly, BEN seeks rescission of the stock and warrant agreements, restitution of all financial benefits obtained by Brewer and AFG, actual damages, exemplary damages, attorneys' fees, and any additional relief deemed appropriate by the Court to fully compensate for the harm caused by Defendants' securities fraud.

### **COUNT 5**

#### **Piercing the Corporate Veil**

#### **(Against Ralph Wright Brewer III)**

160. Plaintiff re-alleges and incorporates by reference each and every allegation set forth above.

161. To pierce the corporate veil and hold an individual personally liable, Plaintiff must demonstrate that the corporate structure was used to perpetrate a fraud, evade legal obligations, or commit other wrongful acts. The individual must have disregarded corporate formalities, used the corporation as an alter ego, and exercised control in a manner that caused harm to the Plaintiff. Here, the facts overwhelmingly support piercing the corporate veil to hold Defendant Ralph Wright Brewer III personally liable for the damages caused to Plaintiff BEN

162. Defendant Brewer dominated and controlled AFG and its affiliated entities—AFG Companies, Inc., AFG Technologies, LLC, CareGard Warranty Services, Inc., Southwest Colonial Reinsurance, Ltd., and Prime Reserve Plus, Inc.—to such an extent that these entities functioned as mere extensions of Brewer himself. Brewer used these corporations as his alter ego, disregarding corporate separateness to achieve personal financial enrichment and perpetrate fraud. By commingling assets, failing to adhere to corporate formalities, and undercapitalizing the



entities, Brewer rendered these corporations incapable of fulfilling their contractual obligations, including those under the Reseller Agreement with BEN

163. Brewer's misuse of the corporate form is evident in his deliberate concealment of AFG's financial instability and operational failures, including the ransomware attack on August 13, 2023. Brewer directed the entities to conceal the attack and misrepresent AFG's compliance with data security standards and operational readiness. These misrepresentations induced BEN to execute the Reseller Agreement and issue millions of dollars' worth of stock and warrants to AFG and Brewer, despite AFG's lack of capacity to meet its obligations. Brewer's fraudulent scheme benefited him personally, as he secured 1.75 million shares of BEN stock and warrants for an additional 1 million shares valued at over \$33.25 million.

164. Brewer also used his control over the AFG entities to repudiate legitimate contractual obligations, such as those under the Consulting Agreements with Due Figlie. Brewer personally directed AFG's refusal to pay Agent Fees and provide equity compensation owed to Due Figlie, despite its full performance under the agreements. Brewer's actions were not isolated or incidental but part of a broader pattern of bad faith conduct aimed at avoiding accountability and maximizing his personal financial gain.

165. In furtherance of his misconduct, Brewer disregarded corporate formalities and undercapitalized the AFG entities, rendering them mere shells incapable of independently meeting their obligations. Brewer commingled corporate and personal funds, using the AFG entities to enrich himself at the expense of BEN and other business partners. This blatant disregard for the corporate form underscores the necessity of piercing the corporate veil to prevent Brewer from shielding himself from liability behind the entities he controlled.

166. Brewer's actions caused significant harm to BEN, including financial losses, reputational damage, and regulatory exposure. BEN issued stock and warrants valued at millions of dollars based on Brewer's fraudulent misrepresentations, only to discover that AFG was incapable of performing under the Reseller Agreement. The concealment of the ransomware attack and AFG's failure to meet data security standards exposed BEN to regulatory scrutiny and forced it to incur substantial costs to mitigate the resulting risks. Brewer's personal misconduct, facilitated through his misuse of the AFG entities, directly caused these damages.

167. Piercing the corporate veil is necessary to hold Brewer accountable for his actions. Brewer's domination and misuse of the AFG entities demonstrate a clear pattern of fraud, bad faith, and intentional harm. Allowing Brewer to escape liability by hiding behind the corporate form would enable him to benefit from his misconduct while leaving BEN and others to bear the financial and reputational consequences.

168. Accordingly, Plaintiff BEN seeks to pierce the corporate veil and hold Brewer personally liable for the damages caused by his actions.

### **COUNT 6**

#### **Civil Conspiracy**

#### **(Against Brewer and All AFG Entities)**

169. Plaintiff re-alleges and incorporates by reference each and every allegation set forth above.

170. A claim for civil conspiracy under Texas law requires proof of (1) a combination of two or more persons, (2) an object to be accomplished, (3) a meeting of the minds on the object or course of action, (4) one or more unlawful, overt acts committed in furtherance of the conspiracy, and (5) damages resulting from the wrongful acts. Here, Defendant Ralph Wright Brewer III and

the AFG entities acted in concert to engage in a coordinated scheme of fraudulent conduct and contractual breaches that caused significant harm to BEN.

171. Defendants Brewer, AFG, AFG Companies, Inc., AFG Technologies, LLC, CareGard Warranty Services, Inc., Southwest Colonial Reinsurance, Ltd., and Prime Reserve Plus, Inc. worked together to defraud BEN and evade their contractual obligations. Their collective objective was to secure substantial financial benefits for Brewer and the AFG entities by inducing BEN to execute the Reseller Agreement and issue millions of dollars in stock and warrants, despite knowing that AFG was incapable of performing under the agreement. This objective included concealing material facts about the ransomware attack, misrepresenting AFG's operational capabilities, and repudiating legitimate contractual obligations owed to BEN and Due Figlie.

172. Defendants reached a meeting of the minds to accomplish this fraudulent objective. Brewer, as CEO of AFG and its affiliated entities, directed and orchestrated the conspiracy. Brewer used his control over the AFG entities to conceal the ransomware attack that occurred on August 13, 2023, misrepresent AFG's compliance with data security standards, and falsely assure BEN that AFG was ready to perform under the Reseller Agreement. The AFG entities, acting under Brewer's direction, actively participated in these fraudulent misrepresentations and omissions, enabling Brewer to enrich himself at BEN's expense.

173. In furtherance of the conspiracy, Defendants committed numerous unlawful, overt acts. These acts included Brewer's deliberate concealment of the ransomware attack, which compromised over 105,000 files and rendered AFG's systems inoperable, and his repeated misrepresentations about AFG's operational readiness and compliance with federal and state data protection laws. Defendants also issued false assurances during the negotiation of the Reseller Agreement, inducing BEN to issue stock and warrants valued at over \$33.25 million. Additionally,

Brewer directed AFG to repudiate the Consulting Agreements with Due Figlie, depriving it of Agent Fees, equity compensation, and other contractual entitlements.

174. As a direct and proximate result of Defendants' conspiracy and wrongful acts, BEN suffered significant damages. These damages include financial losses from the issuance of stock and warrants based on fraudulent representations, lost revenue and strategic opportunities due to AFG's inability to perform under the Reseller Agreement, and substantial costs to address the risks created by AFG's noncompliance and concealment of the ransomware attack. BEN's reputation was also damaged, undermining its ability to secure future partnerships and exposing it to regulatory scrutiny.

175. Defendants' conduct was deliberate, egregious, and carried out in bad faith. Their coordinated efforts to defraud BEN and evade their obligations demonstrate a clear conspiracy to prioritize their own financial interests over their legal and contractual responsibilities. Brewer's statement unbeknown to BEN with his executive leadership in October 2023, declared "We're going to war," underscores his intent to harm BEN and avoid accountability for Defendants' actions.

176. Plaintiff BEN therefore seeks to hold all Defendants jointly and severally liable for the harm caused by their conspiracy.

### **COUNT 7**

#### **Breach of Contract**

**(Due Figlie Claim Against AFG Technologies, LLC, AFG Companies, Inc., and CareGard Warranty Services, Inc.)**

177. Plaintiff reallege each and every allegation set forth above and incorporates them herein.

178. To establish a breach of contract claim under Texas law, the Plaintiff must prove 1) the existence of a valid contact; 2) Plaintiff's performance or tendered performance; 3) Defendants breach of the contract; and 4) damages sustained as a result of the breach.

179. On March 1, 2022, Due Figlie entered into a Consulting Agreement with Automotive Financial Group, Inc. (AFG), represented by its CEO, Ralph Wright Brewer III. Under this agreement, Due Figlie provided consulting services to AFG and played a significant role in generating new business for CareGard Warranty Services, Inc., one of AFG's affiliated entities. On June 1, 2022, the Consulting Agreement was updated to reiterate the terms of the March 2022 agreement.

180. This agreement was supported by mutual consideration: Due Figlie provided its contacts and relationships within the automotive industry as well as years of experience within the automotive industry in return for valuable consideration from AFG.

181. Through its efforts, Due Figlie established new client relationships, increased contract volumes, and contributed to the overall profitability of AFG's operations. These contributions directly benefited Brewer and the AFG entities, aligning with the agreed-upon performance benchmarks.

182. AFG failed to perform its responsibilities under the agreement by failing to provide the compensation called out by the Agreement, including Agent fees and equity compensation including founders share and equity based incentives.

183. As a direct and proximate result of AFG's breaches, Plaintiff BEN suffered substantial financial and reputational harm. Due Figlie has suffered damages including, but not limited, the Agent Fees tied to new business generated for CareGard Warranty Services, the

founder shares and milestone equity compensation, and the reputational harm and lost opportunities arising from failing to honor AFG's contractual obligations.

**COUNT 8**

**Fraudulent Inducement**

**(Due Figlie Claim Against Ralph Wright Brewer III and All AFG Entities)**

184. Plaintiff re-alleges and incorporates by reference each and every allegation set forth above.

185. Fraudulent inducement under Texas law requires proof that a party made a material false representation, knew the representation was false, intended the other party to rely on it, and caused the other party to enter into an agreement that resulted in harm. The facts of this case establish each element of fraudulent inducement.

186. Defendants, led by Ralph Wright Brewer III, made deliberate and material misrepresentations to induce Due Figlie into entering the Consulting Agreements. Brewer specifically represented that Due Figlie would receive considerable equity and payments of Agent Fees in return for the relationships and referrals within the automotive industry by Due Figlie.

187. These representations, however, were patently false and knowingly so. Among numerous other acts and statements, at the time of the signing of the first and second Consulting Agreements, Ralph Wright Brewer III deliberately refused to negotiate milestone equity compensation which illustrates AFG's unwillingness to comply with the terms of the Consulting Agreements.

188. Brewer made these misrepresentations with the specific intent to induce Due Figlie into entering the Consulting Agreements. Brewer and AFG desired the relationships and referrals made by Due Figlie. AFG and Brewer additionally knew at the time of signing the agreements that

AFG would not perform under the agreements but would only pretend to comply with the agreements until the benefits of the relationships and referrals made by Due Figlie were secured by contracts between AFG entities and the parties referred to AFG by Due Figlie. By concealing these facts, Brewer ensured that Due Figlie would execute the agreements under false pretenses.

189. Due Figlie reasonably relied on Brewer's representations in deciding into enter the Consulting Agreements. Brewer, as the CEO of AFG, was in a position of authority and trust, and Due Figlie had no reason to doubt his assurances regarding AFG's intention to provide the compensation due under the Consulting Agreements. These assurances were material to Due Figlies's decision to enter into the agreements and provide the referrals and relationships available to Brewer and AFG in the form of considerable new business. Due Figlie justifiably believed that AFG was capable of fulfilling its obligations.

190. As a direct result of this fraudulent inducement, BEN suffered significant harm. As a direct and proximate result of AFG's breaches, Plaintiff BEN suffered substantial financial and reputational harm. Due Figlie has suffered damages including, but no limited, the Agent Fees tied to new business generated for CareGard Warranty Services, the founder shares and milestone equity compensation, and the reputational harm and lost opportunities arising from failing to honor AFG's contractual obligations. These financial and reputational damages were foreseeable and directly caused by Brewer's deliberate and deceptive conduct.

191. Brewer's actions were intentional, calculated, and egregious. His fraudulent inducement was designed to enrich himself and his affiliated entities at Due Figlie's expense, while deliberately concealing material facts and as a result Due Figlie was irreparably harmed, both financially and reputationally.

## **DAMAGES**

### **Actual Damages**

192. BEN and Due Figlie have suffered significant actual damages as a direct result of the Defendants' breaches of contract, fraudulent conduct, and bad faith actions. These include:

#### **Loss of Anticipated Revenue:**

193. BEN has lost significant anticipated revenue from the Reseller Agreement due to AFG's failure to perform its obligations, including the inability to successfully integrate BEN's AI-powered technology into dealership systems.

194. Due Figlie has been deprived of Agent Fees owed under the Consulting Agreements for the substantial new business it generated for CareGard Warranty Services.

#### **Loss of Equity Compensation:**

195. Due Figlie has been denied founder shares and milestone equity compensation tied to its contributions to Tronix/1Basket, which were essential terms of the Consulting Agreements.

#### **Costs of Mitigation:**

196. BEN has incurred significant costs to mitigate the harm caused by AFG's misconduct, including addressing risks related to the concealed ransomware attack, upgrading IT security, and responding to regulatory inquiries.

### **Consequential Damages**

197. The misconduct of Brewer and the AFG entities has caused cascading harm to BEN and Due Figlie, including:



**Reputational Harm:**

198. BEN's reputation has been significantly damaged due to the Defendants' concealment of the ransomware attack, non-performance under the Reseller Agreement, and Brewer's retaliatory statements to third parties.

199. Due Figlie's reputation has also suffered due to Brewer's repudiation of the Consulting Agreements and refusal to honor its obligations.

**Lost Business Opportunities:**

200. BEN has been deprived of the opportunity to pursue alternative partnerships in the automotive sector that could have advanced its strategic goals.

201. Due Figlie has lost opportunities to expand its consulting business due to the harm caused by Defendants' actions.

**Exemplary Damages**

202. The fraudulent conduct of Brewer and the AFG entities was willful, intentional, and carried out in bad faith, warranting the award of exemplary damages to deter such behavior in the future.

203. Brewer's actions, including his deliberate concealment of the ransomware attack, repudiation of the Consulting Agreements, and declaration of "war" against BEN, demonstrate egregious misconduct deserving of punitive damages.

**Restitution**

204. Restitution is necessary to return BEN to the position it was in before entering into the Reseller Agreement, including the recovery of any financial benefits improperly obtained by Brewer and the AFG entities

**Attorneys' Fees and Costs**

205. BEN and Due Figlie are entitled to recover their attorneys' fees and costs incurred in pursuing this action under applicable law and the terms of the Reseller and Consulting Agreements.

**Pre- and Post-Judgment Interest**

206. BEN and Due Figlie seek pre-judgment and post-judgment interest on all damages awarded, as permitted by law, to fully compensate them for the harm suffered due to Defendants' actions.

Plaintiff BEN and Due Figlie seek judgment against Defendants, jointly and severally, for:

1. Actual and consequential damages, including lost revenue, denied compensation, and mitigation costs.
2. Exemplary damages for fraud, fraudulent inducement, and civil conspiracy.
3. Rescission of the stock and warrant agreements issued to Brewer and AFG, along with restitution of all financial benefits improperly obtained.
4. Attorneys' fees and litigation costs.
5. Pre- and post-judgment interest on all damages awarded.
6. Any additional relief the Court deems just and proper.

Respectfully submitted,

By: /s/ Matthew E. Yarbrough

**MATTHEW E. YARBROUGH**

State Bar No. 00789741

**JASON BLACKSTONE**

State Bar No. 24036227

**ALEXIS N. DEL RIO**

State Bar No. 24120796

**BAKER, DONELSON, BEARMAN,  
CALDWELL & BERKOWITZ, P.C.**

5956 Sherry Lane, 20<sup>th</sup> Floor

Dallas, Texas 75225

Telephone: (214) 466-2738

Facsimile: (713) 650-9701

myarbrough@bakerdonelson.com

jblackstone@bakerdonelson.com

adelrio@bakerdonelson.com

*Attorneys for Plaintiff*